



DO-254 – Complex Hardware Design Assurance

Uma Ferrell

Principal

Ferrell and Associates
Consulting, Inc.

Uma@faaconsulting.com
(703)757-9777

Tom Ferrell

Principal

Ferrell and Associates
Consulting Inc.

Tom@faaconsulting.com
(703)757-9777





Agenda / TOC

- Introductions and Overview
- Hardware Design Lifecycle
- Planning Process
- Hardware Design Process
 - Requirements
 - Conceptual Design
 - Detailed Design
 - Implementation
 - Production Transition
- Supporting Processes
 - Validation and Verification
 - Configuration Management
 - Process Assurance
 - Certification Liaison
- Wrap-up
 - Update and Summary



Abstract

Design Assurance Guidance for Airborne Electronic Hardware

RTCA DO-254/ED-80 (Design Assurance Guidance for Airborne Electronic Hardware) was released in 2000 and is designed to fill the gap for developmental assurance for complex electronic hardware including Programmable Logic Devices (PLDs) and Application Specific Integrated Circuits (ASICs).

This tutorial is intended to provide an introduction to DO-254 and is intended for novice users.





Disclaimers/Copyright

- The material in this presentation is intended to help the student understand and apply DO-254/ED-80 in their development projects. This material represents an interpretation of DO-254 and does not in any way establish policy or guidance.
- No express or implied warranty is provided as to the completeness of this material for supporting certification efforts. It remains the applicant's responsibility for demonstrating compliance to all necessary regulatory requirements throughout the equipment certification.
- Use of the information contained in this presentation is subject to your own judgement. The authors are not responsible for the manner in which this information is used or relied upon.



Document Availability

- DO-254 and ED-80 are copyrighted documents of RTCA and EUROCAE respectively. For the purposes of this presentation, DO-254 shall be used to refer to both the English version and the European equivalent. This convention was adopted solely as a means for brevity.
- Copies of DO-254 may be obtained from:
RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, D.C. 20036 U.S.A
(202)833-9339
- Copies of ED-80 (includes French translation) may be obtained from:
EUROCAE
17, Rue Hamelin
75116 Paris, France
01 45 05 71 88



Scope of DO-254



- Guidance is applicable to, but not limited to:
 - Line Replaceable Units (LRUs)
 - Circuit Board Assemblies
 - **Custom micro-coded components such as ASICs, PLDs, FPGAs, including any associated macro functions.**
 - Integrated technology components, such as hybrids and multi-chip modules
 - Commercial-Off-The-Shelf (COTS) hardware components
- Note: Functions are allocated to either software or hardware during the system definition. DO-254 does not recognize a third class of “stuff” called firmware. The expectation is that you will either use the processes outlined in DO-254 or those in DO-178B to provide comprehensive design assurance.



Document Overview

System
Requirements

FAR/JAR &
Advisory
Materials

System
Development
Guidance

Safety
Assessment
Guidance

Environmental
Qualification
Guidance

DO-254 Contents

Development Constraints:

- System Aspects (Sec. 2)
- HW Design life Cycle (Sec. 3)
- Planning Process (Sec. 4)
- Additional Considerations (Sec. 11)
- Design Assurance for Levels A & B (Appendix B)

Derived Requirements
(as required)

Design Process (Sec. 5)

Supporting Processes:

- V&V Process (Sec. 6)
- CM Process (Sec. 7)
- Process Assurance (Sec. 8)
- Certification Liaison (Sec. 9)

Changes
Required

Production Process

In-Service

Software
Guidance

HW Design Life Cycle Data (Sec. 10)
HW Life Cycle Data by Design Assurance Level and Control Code (App. A)



Adapted from Figure 1-1

Slide 7

2005 Joint FAA/NASA Software and
CEH Standardization Conference

Copyright © 2005 by Ferrell and Associates Consulting, Inc.



Appendix A

- Provides guidance for data and objectives to be satisfied on a level by level basis.
- Not all objectives may be applicable to all assurance levels.
- Identifies data that should be submitted. Some data is identified as “should be available” if referenced in submitted data.
- Certain data items may not be used for “certification credit” and therefore may not be required.
- Identifies configuration control data control category.
- Provides guidance on independence during verification.
 - Organizational independence is not required

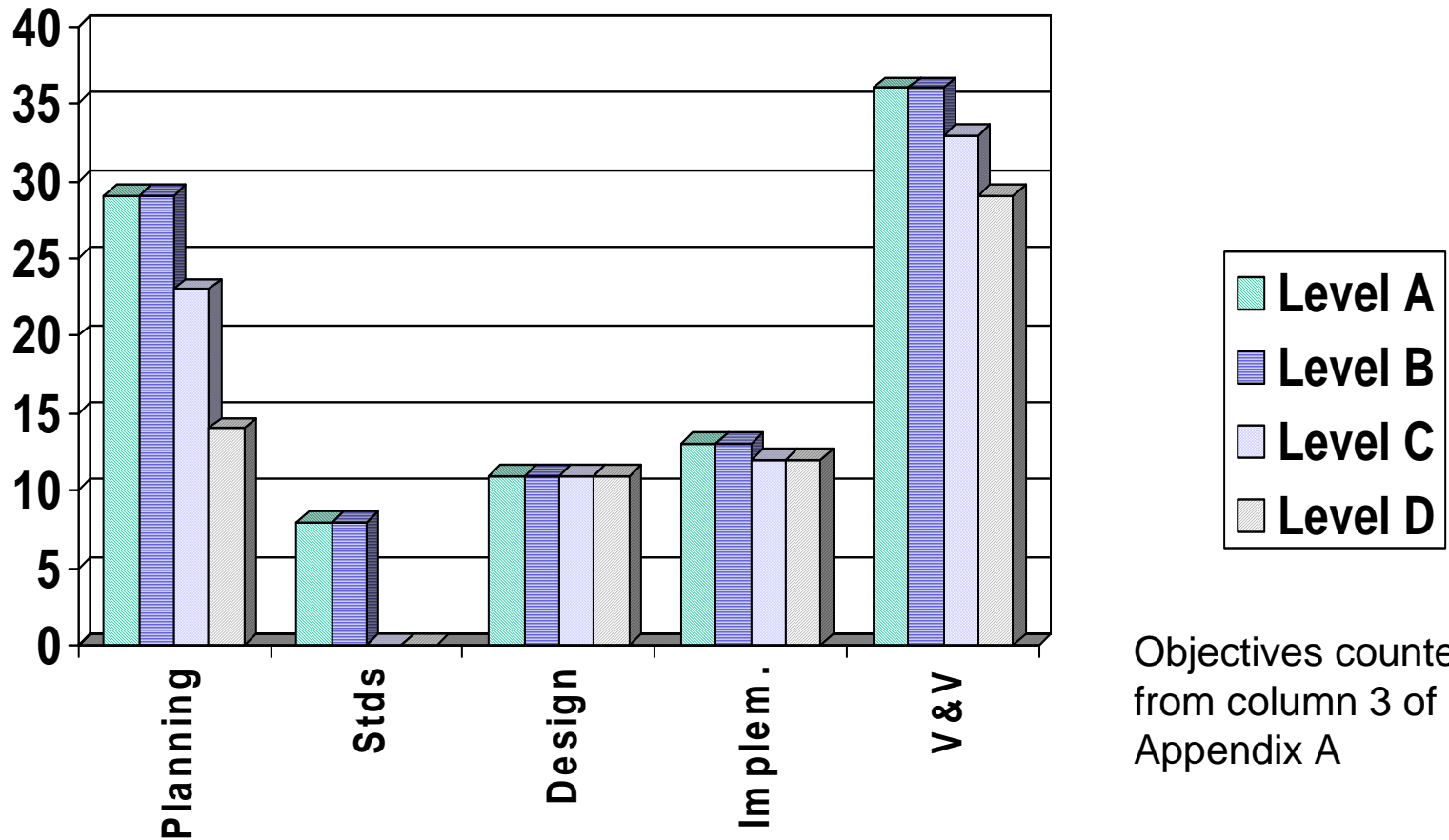


Appendix B

- Provides design assurance considerations for functions of level A and B
- Provides guidance to perform and use a Functional Failure Path Analysis (FFPA) for the purpose of developing a design strategy and guidance on specific design assurance methods
 - Top-down iterative safety assessment strategy
 - Begins with a Preliminary System Safety Assessment (PSSA) to identify system level functional failure paths
 - Fault Tree Analysis is used to decompose the system. Decomposition may be complemented by Functional Failure Modes and Effects Analysis, Dependency Diagrams and Common Mode Analysis.
 - Level of decomposition is subjective. But the goal is to separate functions of higher criticality so that higher level of design assurance have to performed on the least number of functions.
- Discusses additional design and verification assurances methods to support and validate the results of the FFPA.



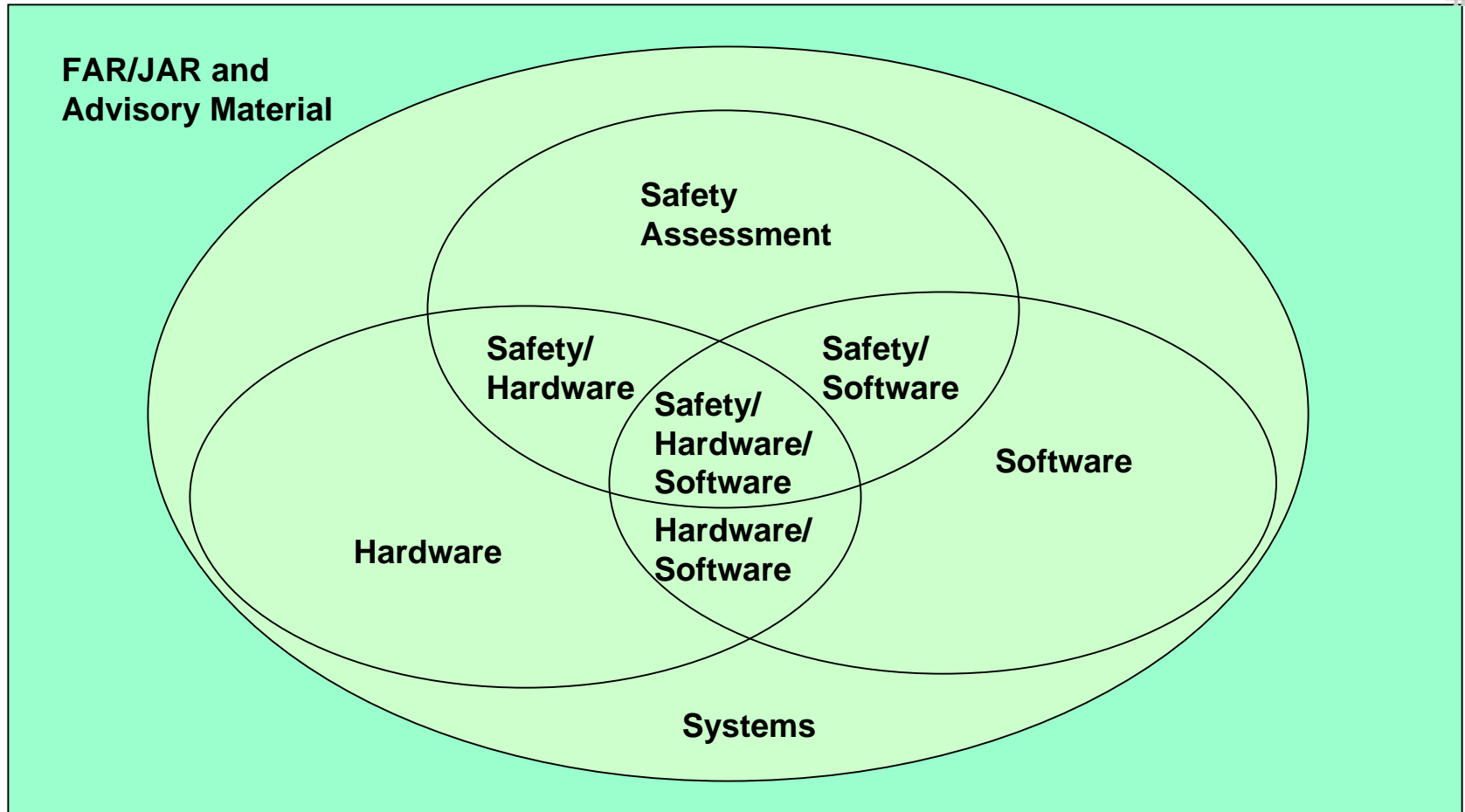
Hardware Design Assurance



Objectives counted
from column 3 of
Appendix A



Relationships between Safety, HW & SW



Adapted from Figure 2-1, DO-254

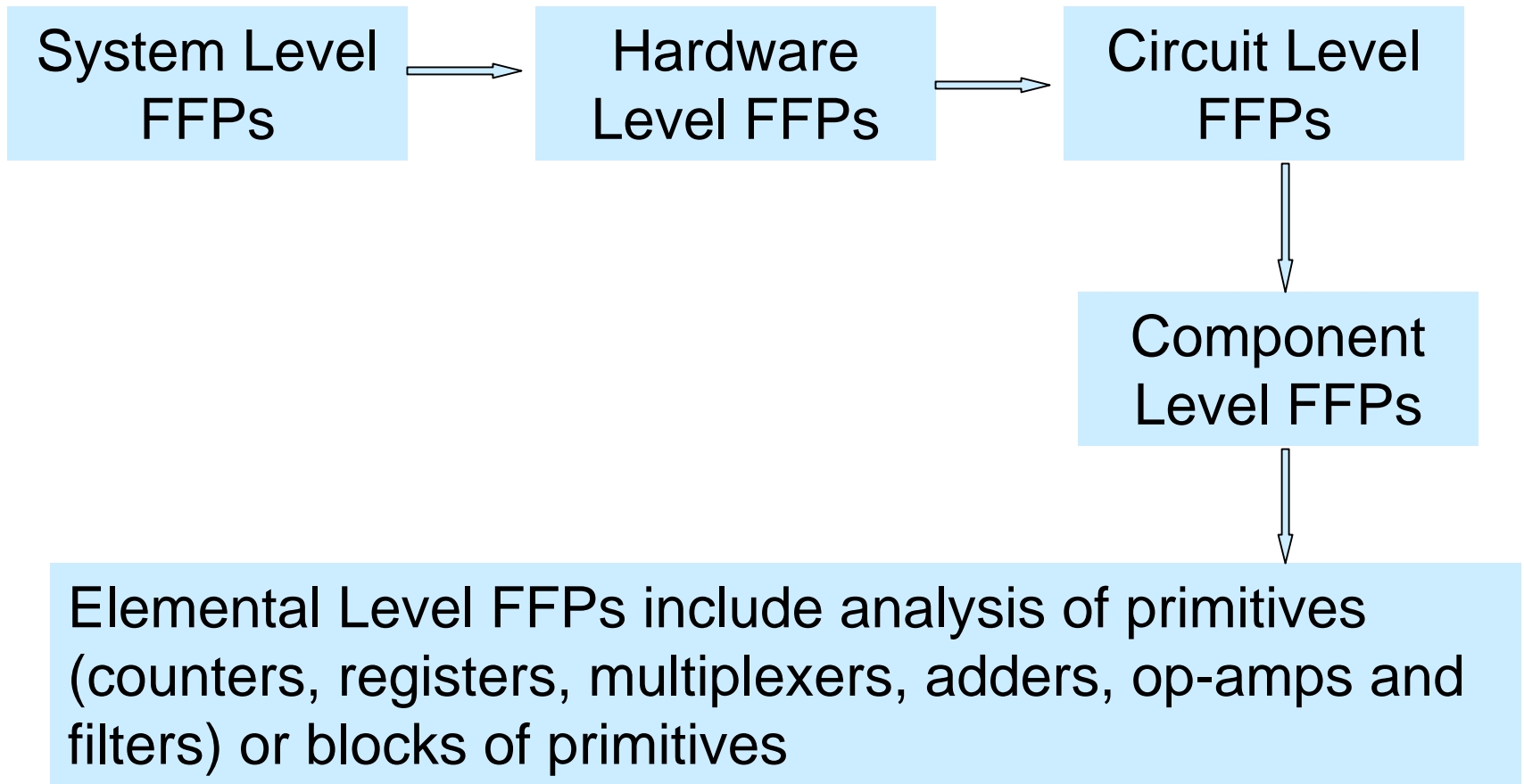
Slide 11

2005 Joint FAA/NASA Software and
CEH Standardization Conference





Functional Failure Path Analysis





Hardware Design Life Cycle

HW Life Cycle - Section 3

- DO-254 does not prescribe any particular life-cycle model.
- Processes noted here may occur in a sequence that is commensurate with the chosen life cycle model and the project specifics.
- Three life-cycle processes:

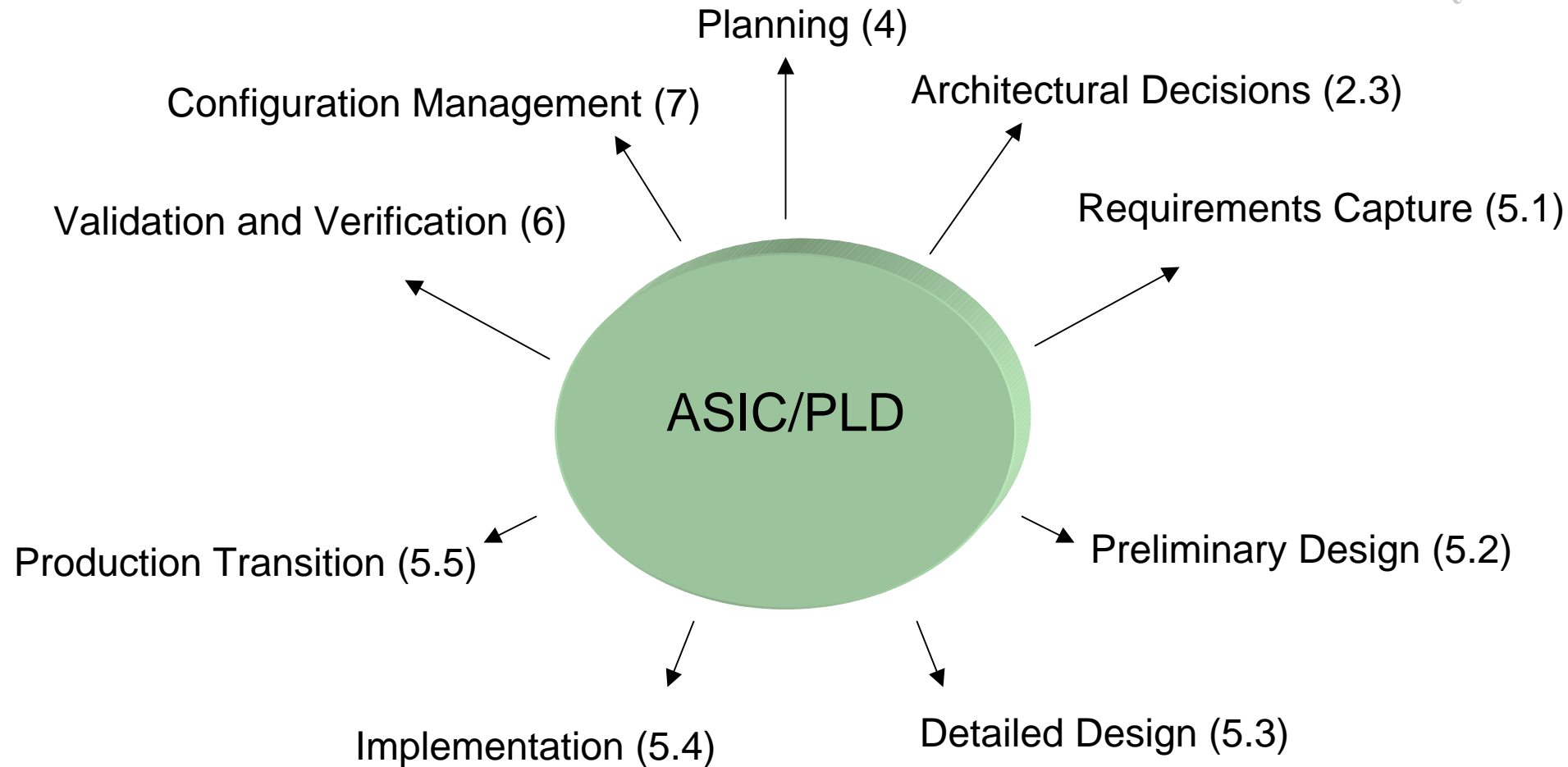
HW Planning Process

HW Design Process

Supporting Processes



The ASIC/PLD Lifecycle





Hardware Planning - The Objectives

- There are four hardware planning process objectives. They are:
 1. The hardware lifecycle processes are defined.
 2. Standards are selected and defined.
 3. The hardware development and verification environments are selected or defined.
 4. The means of compliance of the hardware design assurance objectives, including strategies identified using guidance in Section 2.3.4, are proposed to the certification authority.



Use of Previously Developed Hardware

- Intention to use PDH must be stated in PHAC
- Nature of use of PDH may be
 - modified PDH
 - Change of aircraft installation
 - Change of application or design environment
 - Upgrading a design baseline
- In all of these cases changes to the design from the previous use and configuration control considerations should be noted.
- Guidelines for COTS usage may have some elements that may be used for certification credit for PDH.
- Guidelines for product service history may also be used if applicable.



Commercial Off The Shelf Component Usage

- Use of COTS components is very common in HW designs. Intention to use COTS and means of compliance substantiation should be noted in PHAC.
- Procurement aspects of COTS usage are also discussed in DO-254.
- Use of product service history for credit is encouraged.
- Component manufacturer's track record, quality control, established reliability of the component, technical suitability of intended use, environmental rating, additional testing are all discussed.



Tool Assessment and Qualification

- Tools may be hardware and software to be used during design and verification.
- Design tools generate the hardware item and hence have the capacity to introduce errors in the hardware.
- Verification tools may fail to detect errors in the hardware item or in its design.
- If the tool was successfully used for the same purpose, that history may be applied to current effort.
- Basic tool qualification is that the tool correctly functions.
- Design tool qualification requirements at levels A and B are essentially the same as development tool qualification as documented in DO-178B.



Hardware Design Processes

- DO-254 defines five major design processes: Requirements Capture, Conceptual Design, Detailed Design, Implementation, and Production Transition.

| | | |
|-----------------------|---|--------------|
| Requirements Capture | Hardware Requirements | 3 objectives |
| Conceptual Design | Conceptual Design Data | 3 objectives |
| Detailed Design | Detailed Design Data Top-level Drawing Assembly Drawings Installation Control Drawings Hardware/Software Interface Data | 3 objectives |
| Implementation | | 4 objectives |
| Production Transition | | 4 objectives |



Requirements Capture

The Objectives

The three objectives for the requirements capture process are:

1. Requirements are identified, defined, and documented. This includes allocated requirements from the PSSA and derived requirements from the hardware safety assessment.
2. Derived requirements are fed back to the appropriate process.
3. Requirements omissions and errors are provided to the appropriate process for resolution.



Conceptual Design

The Objectives

The three objectives for the conceptual design capture process are:

1. The hardware item conceptual design is developed consistent with its requirements.
2. Derived requirements produced are fed back to the requirements capture process or other appropriate processes.
3. Requirements omissions and errors are provided to the appropriate process for resolution.



Detailed Design

The Objectives

The three objectives for the detailed design process are:

1. The detailed design is developed from the hardware item requirements and conceptual design data.
2. Derived requirements are fed back to the conceptual design process or other appropriate processes.
3. Requirements omissions and errors are provided to the appropriate process for resolution.



Implementation Process

The Objectives

The four objectives for the implementation process are:

1. A hardware item is produced which implements the hardware detailed design using representative manufacturing processes.
2. The hardware item implementation, assembly, and installation data is complete.
3. Derived requirements are fed back to the appropriate process.
4. Requirements omissions and errors are provided to the appropriate process for resolution.



Production Transition

The Objectives

The four objectives for the production transition process are:

1. A baseline is established that includes all design and manufacturing data needed to support the consistent replication of the hardware item.
2. Manufacturing requirements related to safety are identified and documented and manufacturing controls are established.
3. Derived requirements are fed back to the implementation process or other appropriate processes.
4. Errors and omissions are provided to the appropriate processes for resolution.



Supporting Processes

Hardware Validation and Verification - Section 6

Hardware Configuration Management - Section 7

Process Assurance - Section 8

Certification Liaison - Section 9

The supporting processes can be thought of as an overlay to the life cycle processes. For each step of the life cycle process, there are corresponding activities to be accomplished for validation and verification, configuration management, process assurance, and preparation for certification.



Validation Process

The Objectives

The three objectives for the validation process are:

1. Derived hardware requirements against which the hardware item is to be verified are correct and complete.
2. Derived requirements are evaluated for impact on safety.
3. Omissions and errors are fed back to the appropriate processes for resolution.



Verification Process

The Objectives

The four objectives for the verification process are:

1. Evidence is provided that the hardware implementation meets the requirements.
2. Traceability is established between hardware requirements, the implementation, and the verification procedures and results.
3. Acceptance test criteria are identified, can be implemented, and are consistent with the hardware design assurance levels of the hardware functions.
4. Omissions and errors are fed back to the appropriate processes for resolution.



HW Traceability Data

- Traceability data provides establishes the correlation between all elements of the hardware creation process including requirements, design, implementation, validation, and verification.
- Traceability can be especially problematic given the nature of hardware design documentation.
- To ensure traceability does not become a problem, plan for it up front. Understand how traceability can or will be mechanized via the design tools that you are using. Determining an appropriate level of granularity in your traceability is also helpful
- Always update your traceability data. Avionics hardware has a long lifetime. Good traceability is at the heart of good maintainability (even during iterative development).



Configuration Management (CM)

- Configuration Management is defined as “the process of configuration identification and the control of issues and changes of configuration identities.”
- Configuration Management (CM) must become a habit and should be built into the basic development processes employed on the project.
- Enforcement of CM through tools that provide strict versioning control on drawings, HDL, and related items should help accomplish the CM objectives.

It is important to understand that a significant portion of the governing regulations for aircraft relate to the topic of CM. Once an item is certified all change analysis is performed against the defined configuration.



CM - The Objectives

- The three objectives of the Configuration Management process are:
 - 1 Configuration items are uniquely identified and documented.
 - 2 Consistent and accurate replication of configuration items is ensured.
 - 3 A controlled method of identifying and tracking modification to configuration items is provided.



HW Control Categories

| Configuration Management Activity | HC1 | HC2 |
|---|-----|-----|
| Configuration Identification | • | • |
| Baselines | • | |
| Baseline Traceability | • | • |
| Problem Reporting | • | |
| Change Control – integrity and identification | • | • |
| Change Control – records, approvals, and traceability | • | |
| Release | • | |
| Retrieval | • | • |
| Data Retention | • | • |
| Protection against Unauthorized Changes | • | • |
| Media Selection, Refreshing, Duplication | • | |

Table shows which CM controls are applied to each level. For example, PRs are controlled as a HC2 item, therefore you do not have to write PRs on problems noted in other PRs.

Adapted from Table 7-1, DO-254



HW CM Records

- Hardware CM records are the day-to-day results of an active configuration management process.
- Records should include:
 - Configuration Identification Lists
 - Baseline records
 - Change History Reports
 - Problem Report Summaries
 - Tool Identification Records
 - Archive Records
 - Release Records

Many of the CM records are likely to reside in a central database which provides CM support to the entire development team. Others will be found in the corporate engineering control system. The CM plan should note the location of the various records discussed in DO-254.



Process Assurance

The Objectives

- Three objectives must be satisfied for process assurance for levels A, B, and C hardware:
 - Life cycle processes comply with approved plans.
 - Hardware design life cycle data produced complies with the approved plans.
 - The hardware item used for conformance assessment is built to comply with the associated life cycle data
- In addition, note that the hardware process assurance records must also contain evidence of the second CM objective:
 - Consistent and accurate replication of configuration items is ensured.



Hardware Conformity

- The ultimate goal of the conformity process is to ensure that the AS-DELIVERED product matches the AS-BUILT/AS-VERIFIED product.
- DO-254 discusses hardware conformity in terms of a final review as the last step to close-out the hardware portion of a certification application. Conformity can and should be used throughout the development effort.
 - Data items about to undergo a final inspection for credit should be conformed (i.e., item clearly identified with a version number and under configuration control).
 - Hardware ready for final test or to be used in certification testing of the software or system should be conformed [e.g., a Conformed Test Article (CTA)].



Certification Liaison

- Although specific objectives for this process are not provided, four guidance items are stated:
 - The data required to be submitted should be provided for review early, i.e. at a time when impacts of design changes would be minimal.
 - Issues raised by the certification authority should be resolved.
 - Agreement on the contents of the PHAC should be obtained.
 - Communication with the certification authority should continue throughout the development cycle with any issues raised being resolved in a timely manner.



The Hardware Accomplishment Summary

- The PHAC told the certification authority what you were going to do. The Hardware Accomplishment Summary tells them what you actually did.
- The Hardware Accomplishment Summary contents covers the following areas:
 - System Overview
 - Certification Considerations
 - Hardware Life Cycle Data
 - Additional Considerations
 - Hardware Overview
 - Hardware Design Life Cycle Description
 - Previously Developed Hardware
 - Alternative Methods
- This document must also identify differences from the approved PHAC and contain identification information for the hardware, the change history and status of the hardware, and finally, a compliance statement.



The New AC

- AC 20-152 was released at the end of June (2005).
- The AC alters the application of DO-254 in fundamental ways:
 - Scope is limited to complex devices ONLY – application of DO-254 to complete Line Replaceable Units (LRUs) and Circuit Card Assemblies (CCAs) is no longer required
 - Application at level D is optional and not subject to FAA oversight/approval
 - Strengthens exemption for Commercial-Off-The-Shelf (COTS) microprocessors
- The AC is applicable for every form of certification [e.g., Type Certification (TC), Technical Standard Order (TSO) authorizations, Parts Manufacturer Approval (PMA)]





Summary

- DO-254 provides a comprehensive set of guidelines for design assurance activities for use during the development of complex electronic hardware.
- The standard loosely parallels DO-178B, the industry standard for design assurance for software.
- As with any standard, particularly new ones, expect to find some inconsistencies and apparent omissions.
- Before using DO-254 on a project, make sure you have an agreement with your certification authority as to exactly how and to what DO-254 will be employed for your project.
- Feedback your experiences with DO-254 to RTCA or the FAA so that future revisions can be improved.





Additional Sources (1)

- RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware* (see slide 5)
- FAA AC 20-152, *RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware*
- *Complex Electronic Hardware Interactive Video and Self-Study Course* available at <http://av-info.faa.gov/software/complexhdw.html>
- *Design, Test, and Certification Issues for Complex Integrated Circuits*, DOT/FAA/AR-95/31 Technical Report available at:
 - Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(800) 553-6847



Additional Sources (2)

- *An Introduction to VHDL*, David Pellerin, Accolade Design Automation available at http://www.acc-eda.com/h_intro.html
- Application Specific Integrated Circuits, Smith, Addison-Wesley Longman, 1997
- *RTCA DO-178B, Software Considerations for Airborne Systems and Equipment* (see slide 5)
- *RTCA DO-160D, Environmental Conditions and Test Procedures for Airborne Equipment* (see slide 5)
- *ARP 4754, Certification Considerations for Highly Integrated or Complex Aircraft Systems*, SAE, <http://www.sae.org>
- *ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, SAE, <http://www.sae.org>